A propos de l'avis de la commission de protection de la vie privée du 15 juin 2005 sur l'encadrement des listes noires

Burton, Cedric; Poullet, Yves

Published in:
Défis du droit à la protection à la vie privée

Publication date:
2008

Document Version
le PDF de l'éditeur

À PROPOS DE L'AVIS DE LA COMMISSION DE PROTECTION DE LA VIE PRIVÉE DU 15 JUIN 2005 SUR L'ENCADREMENT DES LISTES NOIRES (1)

Cédric BURTON
Avocat au Barreau de Bruxelles

et

Yves POULLET
Directeur du Centre de Recherches Informatique et Droit,
Professeur aux Facultés de droit de Namur et Liège

Sommaire : I. Qu'est-ce qu'une liste noire ? I.1. Liste noire, une notion ambiguë et un débat délicat. *I.1.1. Des frontières mal établies. I.1.2. Tentative de définition.* I.2.Analyse des intérêts poursuivis par les listes noires et des dangers créés par elles. *I.2.1. Des arguments en faveur des listes noires. I.2.2. Des arguments contre les listes noires. I.2.3. De la nécessité d'une balance.* II. Rappel des principes applicables aux listes noires. La LVP est-elle suffisante ? II.1.Conditions de légitimité du traitement et de son contenu imposées au responsable du traitement. II.1.1. Légitimité quant à l'existence du traitement. II.1.2. Consentement légitimant le traitement. II.1.3. Principe de proportionnalité : de la mise en balance de l'intérêt légitime du responsable du traitement et de l'intérêt du fiché. *II.2.1. Légitimité quant au contenu du traitement. II.2.2. Le cas particulier des données judiciaire.* II.2.2.1.L'article 8, un article flou aux contours incertains. II.2.2.2. Des suspicions [...] ayant trait à des infractions ? II.2.2.3. Dans un cadre judiciaire ! II.2.2.4. Du champ de la notion d'infraction. II.2.2.5. Des causes de légitimité particulières aux données judiciaires. *II.3. Des droits de la personne concernée et des obligations corrélatives du responsable du traitement.* II.3.1. Droit d'information. II.3.2. Droit d'accès. II.3.3. Les systèmes de décisions automatisées. II.3.4. Principe de sécurité : des obligations existantes... mais peu respectées. III. Faut-il légiférer en la matière ?. *III.1. Les fondements possibles d'une intervention législative. III.2. Quel contenu ?*

Résumé : À partir d'un avis récent de la Commission belge de protection de la vie privée, la contribution analyse dans une perspective de droit comparé la façon optimale de réglementer les listes noires qui se multiplient dans nos pays. Elle tâ-

(1) Commission pour la protection de la vie privée, 15 juin 2005, avis n° 09/2005 sur un encadrement des listes noires.

che d'établir les conditions d'un juste équilibre entre les intérêts des entreprises et ceux des citoyens. Si les principes essentiels de la Directive 95/46 de l'Union européenne constituent une base de travail importante en la matière, sans doute les risques accrus de discrimination injustifiée ou erronée justifient une attention particulière et l'octroi de droits nouveaux aux personnes concernées de même que la fixation de conditions supplémentaires pour les responsables de traitement.

Abstract : Apart from a recent opinion delivered by the Belgian Data Protection authority about the blacklistings, the article intends in a comparative law perspective to determine the best way to regulate these processing, which are more and more frequent in our countries. The contribution aims to establish the conditions of a fair balance between the companies' interests from one side and the citizens' ones. If the EU Directive 95/46 essential principles might be considered as a good point of departure for founding this adequate balance it seems due too the increased risks of unjustified or erroneous discrimatory practices that complementary rights must be granted to the Data subjects and that severe limitation ought to be imposed to the Data controllers.

L'existence de ce type de fichier n'est pas un phénomène nouveau, mais de nos jours, cette pratique tend à s'étendre. Assurances, banques, associations patronales, associations de propriétaires, grandes surfaces, salles de jeux, fournisseurs de téléphonie ou autres fournisseurs de communications électroniques, etc (2) constituent autant d'acteurs utilisant ce que l'on appelle communément des listes noires. Le législateur (3) semble vouloir s'emparer de cette délicate question afin d'encadrer les pratiques actuelles. Saisie par Madame la Ministre de l'emploi, la Commission de protection de la vie privée (CPVP) a émis, le 15 juin, un avis sur la nécessité et le contenu d'un encadrement législatif des listes noires.

L'article analyse ces pratiques au regard de la législation de protection des données à caractère personnel (4), écartant volontairement les questions posées par les listes noires vis-à-vis du droit de la concur-

(2) Cette liste n'est qu'illustrative, a titre d'exemples d'autres listes noires existent : les avocats et architectes utilisent des listes de mauvais-payeur ; certains journaux publient des listes de pédophiles ou de coureurs dopés ; Test-achats publie des listes de firmes douteuses ; les États européens et bientôt la Commission publieront des listes noires de compagnies d'aviation, etc…

(3) Voy. Proposition de loi modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel en ce qui concerne les conditions générales de licéité des traitements de données à caractère personnel, *Doc.parl.*, Ch. repr., sess. ord. 2004-2005, n°1693/001 du 31 mars 2005. Egalement disponible sur le site de la Chambre des représentants : http://www.lachambre.be

(4) Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, p. 5801. Pour toutes les références ultérieures à ce texte, nous utiliserons LVP.

rence (5). Dans un premier temps, nous tenterons de définir la notion de liste noire. Ensuite, seront passés en revue certains principes présents dans la législation de protection des données personnelles permettant d'encadrer, potentiellement du moins, ce phénomène. Pour finir, nous émettrons de brèves réflexions sur l'opportunité d'une intervention de l'État, le mode de régulation et son contenu. Cet avis nous offre également l'occasion d'éclaircir la notion de données judiciaires ou, pour être plus précis, de préciser le champ d'application de l'article 8 de la loi du 8 décembre 1992.

I. Qu'est-ce qu'une liste noire ?

I. 1. Liste noire, une notion ambiguë et un débat délicat

I.1.1. Des frontières mal établies

La notion de liste noire est large et difficile à cerner avec précision. Une typologie utilisant comme critère distinctif les acteurs pouvant accéder aux données de la liste noire permet de dégager l'extension de cette notion. Premièrement, les fichiers internes sont à différencier des fichiers externes. Ensuite, au sein de cette dernière catégorie, trois nouvelles sous-catégories peuvent être dénombrées.

– Les **fichiers internes** c'est-à-dire les fichiers utilisés par une seule entreprise et dont la base de données ne sera utilisée et accessible que par l'entreprise gérant cette base de données.

– Les **fichiers externes** c'est-à-dire les fichiers destinés à être alimentés et consultés par des entités plus nombreuses qu'une seule entreprise. Dans une majorité de cas, la base de données sera alimentée par chaque entreprise (responsable du traitement) et la gestion proprement dite de celle-ci sera attribuée à un sous-traitant. Suivant notre critère, les listes seront accessibles :

i. soit uniquement à un groupe d'entreprises (par exemple à l'ensemble des entités du groupe Dexia, Axa ou autre…),

ii. soit l'entièreté d'un secteur (6) (comme c'est le cas du fichier Datassur pour les assureurs ou du fichier Préventel pour les opérateurs de mobilophonie, les listes propres au secteur de la

(5) Sur ces questions, voy. J. Laffineur, « Listes noires ou décisions blanches ? », *D.C.C.R*, 2004, n° 65, p.12.

(6) Pour une liste d'initiatives relatives à des listes noires dans le secteur des assurances, voy. J. Dhont, « Le traitement de données à caractère personnel dans le secteur d'assurances. La légalité des banques de données », *Rev. dr. U.L.B.*, n° 21, 2000, pp. 320 et s.

grande distribution ou celles tenues par la Banque nationale ou l'UPC accessibles aux institutions du secteur du crédit à la consommation, etc..),

iii. et enfin, à plusieurs secteurs. Ces listes multisectorielles voire universalistes ont pour but de rassembler l'ensemble des informations sur une personne donnée tout secteur confondu ou de les rendre accessibles de manière large (par exemple, les listes noires de coureurs dopés sur internet, ...) (7).

I.1.2. Tentative de définition

Dans un langage courant une liste noire est un « *fichier recensant des personnes indésirables* » (8) ou d'après la définition du petit Robert, « *une liste de gens à surveiller, à abattre* ». Quant à la CPVP (9), elle se range derrière la définition donnée par le Groupe dit de l'article 29 (10) : « *Les listes noires consistent à collecter et à diffuser certaines informations concernant un groupe donné de personnes, élaborées conformément à certains critères en fonction du type de liste noire dont il s'agit,* ***se traduisant en règle générale par des effets nocifs et préjudiciables pour les personnes qui y figurent****. Ces effets peuvent entraîner la discrimination d'un groupe de personnes en les* ***privant de toute possibilité d'accès à un service déterminé ou en nuisant à leur réputation*** ».

La première partie de cette définition se contente de spécifier un traitement de données à caractère personnel. Par la suite, le Groupe 29 avance son seul critère permettant de distinguer les listes noires des traitements de données 'classiques', celui **d'effet nocif et préjudiciable pour les personnes y figurant** et fait allusion à deux des finalités des listes noires : la restriction de l'accès à un service déterminé

(7) Nous évoquons ici la question des listes noires largement publiées y compris sur Internet et dont le but est de « moraliser un secteur de la vie sociale ». On songe bien évidemment à la publication de la liste des sportifs surpris en état de dopage, liste dont un décret de la Communauté flamande décidait la création. Ce décret a été sévèrement critiqué par la Cour d'arbitrage (Cour d'arbitrage, Arrêt 16/2005) au nom de l'article 22 de la Constitution consacrant le droit fondamental des citoyens à la vie privée.

(8) Commission Nationale de l'Informatique et des Libertés (CNIL), Rapport sur les listes noires, *Documentation française*, novembre 2003, p. 5, disponible sur http//Les rapports. ladocumentationfrancaise.fr.

(9) Avis cité, point 4.1.1.

(10) Le Groupe instauré par l'article 29 de la directive 95/46/CE (Dir. 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, art. 29, *J.O.C.E.*, L 281, du 23 novembre 1995, p. 0031 à 0050), appelé dans la suite de l'article « groupe de l'article 29 », a émis un document de travail n° 65 sur les listes noires le 3 octobre 2002, 11118/02/FR/final, avis disponible sur le site de la Commission européenne à l'adresse : http://europa.eu.int/comm/justice_home/fsj/privacy/studies/index_en.htm

et la nuisance à la réputation d'une personne. Cette définition est à nos yeux lacunaire car elle aborde le problème par le contenu. De plus, par sa largesse, tout traitement de données à caractère personnel est susceptible de tomber dans cette définition (11) car la référence aux finalités n'est qu'implicite et secondaire alors qu'elle devrait être le critère déterminant (12).

C'est d'ailleurs ce critère que la CNIL utilise dans son rapport pour distinguer les listes noires. Elle y avance les classifications suivantes (basées sur une finalité réelle ou déclarée) : obtenir le règlement de la créance ou écarter les mauvais payeurs et écarter les clients à risques. Sur cette base, nous proposons de définir les listes noires comme des « **fichiers constitués de données à caractère personnel dont la finalité est** *soit* **d'obtenir le règlement d'une créance ou de constater son non-paiement,** *soit* **de constater des anomalies,** *soit* **d'écarter des clients représentant un risque pour un ou plusieurs secteurs, l'entreprise ou le particulier** *soit* **de nuire à la réputation d'une personne** ». La notion de risque devra s'interpréter de façon extensive et vise par exemple le risque de vol, fraude, faux, risque aggravé, etc..

Cette définition permettrait d'appréhender certaines listes pouvant prêter à interprétation si on utilise la définition restrictive du Groupe de l'article 29. Ainsi, selon notre opinion, une liste de personnes ne désirant pas recevoir de polluriels pourrait se voir qualifiée ou non de liste noire suivant les finalités. Si le but de cette liste est d'exclure ces personnes d'un service en posant comme condition d'accès à ce service l'acceptation de messages publicitaires, on doit, selon nous, la qualifier de liste noire. Si par contre cette liste est conservée par un fournisseur d'accès ou de services pour, par exemple, appliquer des filtres spéciaux aux boîtes de réception qu'il héberge, la qualification de liste noire ne pourra pas être retenue.

De plus, en évitant de définir une liste noire par son objet nous évitons d'écarter certaines listes positives qui utilisées négativement seront qualifiées de listes noires. Par exemple, une liste positive (ou blanche) de personnes payant effectivement les remboursements de crédits qu'elles ont contractés peut aussi avoir des effets préjudiciables. Il suffit pour l'entreprise responsable de la liste de vérifier si la personne, cliente chez elle, est présente sur la liste positive pour, *a*

(11) En effet, la première phrase de cette définition pourrait comprendre tout traitement de données à caractère personnel car il est possible d'argumenter que par nature tout traitement de données à un caractère privacide et donc emporte des effets négatifs pour la personne fichée.

(12) Quant à la deuxième phrase de cette définition ; elle cite deux des finalités des listes noires et donc potentiellement exclut toutes les autres listes noires présentant des finalités autres bien que le terme « peuvent » fait référence à une liste ouverte.

contrario, savoir qu'elle n'est pas un 'bon payeur' si elle n'y figure pas. Un même effet pourrait donc être atteint aussi bien par une liste blanche utilisée de façon négative que par une liste noire consultée positivement. En résumé, ce qui caractérise une liste noire est l'utilisation qui va être faite des données qu'elle contient (et non son contenu) et par conséquent la finalité du traitement.

Cette approche par les finalités nous amène à poser la question suivante : faut-il traiter de la même manière les « listes noires » dont la finalité est de prévenir la fraude et celles dont la finalité est de constater la non-exécution d'un simple devoir contractuel, c'est-à-dire le non paiement d'une obligation. Ne devraient-elles pas se voir appliquer un régime particulier ? Les deux finalités ne doivent-elles pas être distinguées ? Le risque de voir apparaître des « casiers judiciaires privés » encourage la prise de garanties supplémentaires pour ce premier type de fichiers. Y invite en outre, mais nous reviendrons sur ce point, la disposition particulière de l'article 8 de notre loi qui prévoit un régime particulier pour les données dites « judiciaires ».

I. 2. ANALYSE DES INTÉRÊTS POURSUIVIS PAR LES LISTES NOIRES ET DES DANGERS CRÉÉS PAR ELLES

La légitimité de la pratique des listes noires réside dans la multitude d'intérêts divergents à prendre en considération. Une mise en balance des avantages et inconvénients doit être opérée (13) car ces pratiques sont à la fois nécessaires pour le secteur industriel afin de se prémunir contre certains clients, apprécier le montant demandé en échange de certains services et, parallèlement, faute d'encadrement, elles peuvent rapidement se montrer « privacides ». Dans les paragraphes qui suivent, nous allons tenter de lister quelques arguments souvent invoqués « pour et contre » les listes noires.

I.2.1. Des arguments en faveur des listes noires

Premièrement, les responsables de traitement avancent souvent les arguments suivants à propos de leurs propres listes noires : soumises à la loi du marché, les entreprises doivent, pour être concurrentielles proposer les prix les plus bas possibles. Pour fixer ce prix, un calcul du risque que représente le client est nécessaire. À cette fin, elles ont un intérêt légitime de se protéger contre les clients à risque, ceci représentant pour eux une nécessité économique (14). De plus, la liberté

(13) Voir à ce propos, l'avis très nuancé du Groupe de l'article 29 déjà cité.

(14) « Le système d'assurance basé sur la solidarité organisée entre assurés, ainsi que la concurrence nécessitent que les assureurs puissent évaluer le risque économique qu'ils encourent », J.

d'entreprise et du commerce leur permet dans une certaine mesure de gérer librement leur affaire. L'obligation légale d'information (15) qui s'impose aux compagnies d'assurance doit également être signalée. Celle-ci les oblige à contrôler les données transmises par le candidat à l'assurance afin de leur permettre « d'une part, d'apprécier correctement le risque et de faire une prime équitable pour tous et, d'autre part, de lutter contre la fraude à l'assurance » (16). Ces finalités ont d'ailleurs été considérées comme légitimes par le juge des référés du tribunal de Bruxelles dans une affaire Datassur (17), nonobstant l'avis de la Commission de protection de la vie privée (18).

Au delà de l'entreprise, un secteur tout entier peut avoir un intérêt légitime à se protéger contre les débiteurs défaillants et les pratiques frauduleuses dont sont victimes leurs membres qui, si elles se répandaient, pourraient remettre en cause le bon fonctionnement de l'ensemble du secteur et compromettraient les intérêts de la clientèle du secteur voire l'image de marque d'un secteur considéré comme insuffisamment attentif à bien sélectionner sa clientèle. Citons par exemple, les listes noires des établissements de jeux de hasard empêchant l'accès aux personnes suspectées de tricherie à ce type d'établissement ou celles du secteur mobilophonique faisant la chasse aux fraudeurs .

Finalement, du côté des personnes fichées, la pratique présente aussi certains avantages. Dans le secteur du crédit par exemple, elle permet de lutter contre le surendettement en offrant aux éventuels nouveaux prêteurs la possibilité de consulter l'état d'endettement du candidat. À titre d'illustration, nous pouvons citer la réglementation concernant la Centrale des Crédits aux Particuliers (19). Cette réglementation met en place deux volets, l'un dit positif et l'autre dit négatif. Le volet négatif vise l'enregistrement de tous les contrats de

---

DHONT, « Le traitement de données à caractère personnel dans le secteur d'assurances. La légalité des banques de données », *Rev. dr. U.L.B.*, n° 21, 2000, pp. 320 et s.

(15) Loi du 25 juin 1992 sur le contrat d'assurance terrestre, art. 5, *M.B.*, 20 août 1992, p. 18283.

(16) Civ. Bruxelles (réf), 19 décembre 2000, *Bull.ass.*, 2001, p. 266, note VAN OLDENEEL, C.-A., pp. 277 à 281 ; voy. également B. DUBUISSON, « Secrets, mensonges et confidences – Conclusions », *Rev. dr. U.L.B.*, n°31, 2000, p.364.

(17) Civ. Bruxelles (réf), 19 décembre 2000, *op. cit.* ; Civ. Nivelles (réf), 28 mars 2003, inédit ; Civ. Brugges (réf.), 31 octobre 2001, inédit ; Civ. Bruxelles (8° ch.) (réf.), 11 juin 2004, inédit.

(18) Commission de la protection de la vie privée, Avis d'initiative n° 21/2000 relatif au fichier RSR (fichier ayant pour but le signalement, entre compagnies d'assurance, des risques spéciaux en assurances incendie, accidents et risques divers) géré par le Groupement d'intérêt économique Datassur.

(19) Loi du 10 août 2001 relative à la Centrale des Crédits aux Particuliers, *M.B.*, 25 septembre 2001, p. 32027 et arrêté royal du 7 juillet 2002 réglementant la Centrale des Crédits aux Particuliers, *M.B.*, 19 juillet 2002, p. 32542.

crédit à la consommation et de tous les contrats de crédit hypothécaires qui connaissent des défauts de paiement. Le volet positif quant à lui vise l'enregistrement de tous les contrats à la consommation et de tous les contrats de crédit hypothécaire souscrits. Préalablement à la conclusion de nouveau contrat de crédit, les entités concernées consulteront ces bases de données afin d'obtenir une information complète sur l'existence éventuelle d'autres contrats de crédit et leur hypothétique défaut de paiement. Ce système fondé sur une double liste permet de lutter contre le surendettement en permettant au prêteur de juger du niveau de solvabilité, d'endettement de l'emprunteur.

I.2.2. Des arguments contre les listes noires (20)

Comme le relève la Commission, les listes noires comportent certains aspects négatifs :« (1) la masse de données enregistrées dans certaines banques empêche un contrôle réel et efficace de la qualité des données ; (2) des violations de confidentialité et l'absence d'identification de leurs auteurs sont rendues possibles par une sécurité insuffisante et/ou un manque de formation des participants, particulièrement dans le chef des interlocuteurs directs (« au guichet ») avec la personne fichée; (3) le fichage est détourné de sa finalité originelle. Une liste noire créée pour une finalité déterminée (par exemple, la lutte contre le surendettement) est également utilisée comme moyen de contrôle à l'égard des candidats à un emploi ; (4) les erreurs humaines fréquentes dues à la complexité du système en place, l'inadéquation du système ». On notera que les dispositions de la LVP, à condition qu'elles soient effectivement appliquées, permettent de résoudre ces différents problèmes comme nous le démontrerons plus bas.

Dans certains cas, les risques sont démultipliés par des facteurs aggravants tels la mutualisation ou l'exclusion de service répondant à des besoins ou droits fondamentaux. Les risques sont alors de « ***stigmatiser*** une catégorie de la population qui peut rencontrer des difficultés parfois passagères, telles que la perte d'un emploi, une maladie grave, une évolution de la situation familiale,…», ***d'exclure*** une partie de la population de services, de « besoins ou d'intérêts considérés comme essentiels à la vie en société », « ***d'affecter,*** potentiellement, les intérêts d'une catégorie de citoyens en protégeant les intérêts d'une autre catégorie » (21).

(20) Les associations de consommateurs se saisissent régulièrement du problème, voy. par exemple, « Des assurés fichés sans contrôle! », *Test-achats*, 1er juillet 2000, disponible sur http://www.testachats.be/images/19/194821_attach.pdf.

(21) Commission pour la protection de la vie privée, 19 avril 2002, avis n° 52/2002 relatif à la constitution d'un fichier externe des locataires défaillants, disponible sur http://www.moniteur.be.

I.2.3. De la nécessité d'une balance

De cet aperçu de la divergence d'intérêts à propos des listes noires nous déduisons qu'une délicate mise en balance d'intérêts est nécessaire. Cet arbitrage devra être réalisé entre d'une part les aspects positifs de ces fichiers et d'autre part les dangers que ceux-ci peuvent représenter, notamment pour la vie privée. Actuellement, une telle mise en balance doit, selon le prescrit de l'article 5 f.) de la LVP, être réalisée *a priori* par le responsable du traitement et ce sous le contrôle *a posteriori* du juge en cas de litige (22). Étant donné l'ampleur que peuvent atteindre de tels traitements et les droits pouvant être affectés, ces garanties suffisent-elles ?

On ajoutera que cette mise en balance n'est pas simple (23) : la constitution d'une liste noire dans le secteur bancaire ou dans un secteur relatif à la fourniture d'énergie sera évaluée différemment s'il existe dans ce secteur pour la personne menacée d'exclusion le droit à réclamer un service minimal bancaire ou de fourniture d'énergie.

II. RAPPEL DES PRINCIPES APPLICABLES AUX LISTES NOIRES. LA LVP EST-ELLE SUFFISANTE ?

Dans l'état actuel du droit, la LVP permet déjà d'encadrer cette pratique. En effet, à condition de rentrer dans son champ d'application, principe de finalité, de légitimité, de loyauté, de proportionnalité et d'exactitude, droit d'information, d'accès et de rectification, obligation de déclaration, obligation de sécurité, ... sont autant d'outils permettant d'encadrer les listes noires. Certains points méritent cependant que l'on s'y attarde.

II.1. CONDITIONS DE LÉGITIMITÉ DU TRAITEMENT ET DE SON CONTENU IMPOSÉES AU RESPONSABLE DU TRAITEMENT

II.1.1. Légitimité quant à l'existence du traitement

Le principe de légitimité du traitement permet d'encadrer les listes noires dans la mesure où d'une lecture combinée des articles 4 et 5 de la LVP, le fondement de légitimité d'un traitement doit rentrer néces-

(22) Cf. également le principe de proportionnalité sous-tendant l'article 4, 3 de la LVP « *§1. Les données à caractère personnel doivent être : 3° adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement* ».

(23) Pour illustrer la difficulté de cette mise en balance, comparez les conclusions sur la légitimité du traitement de la Commission de la protection de la vie privée dans son arrêt Datassur, *op. cit.* et en sens opposé, les conclusions du juge dans l'affaire Datassur, Civ. Bruxelles (réf), 19 décembre 2000, *op. cit* .

sairement dans l'une des six hypothèses prévues par la loi. En ce qui concerne les listes noires internes, le point 5, b), permettra de justifier la liste noire dans un bon nombre de cas dans la mesure où le traitement sera jugé comme nécessaire à la bonne exécution du contrat, ainsi la banque qui enregistre ses mauvais clients le justifiera par les nécessités du contrat et de son bon déroulement, de même si un bailleur enregistre le défaut de paiements des loyers qui lui sont dus.

Par contre, dans le cadre des listes externes, invoquer ce fondement de légitimité apparaît difficile à soutenir. D'autres bases de légitimation pour les listes noires externes sont alors à chercher et, comme la CPVP l'identifie, les responsables de traitement invoquent régulièrement le point « a » et « f » de l'article 5 LVP. Nous allons donc nous attarder sur ces deux bases de légitimité.

II.1.2. Consentement légitimant le traitement (24)

Sur la notion de consentement comme fondement de légitimité

Le consentement permet-il de légitimer un traitement de données dans le cadre de listes noires ? Notons d'abord que cela dépend des données traitées. Des régimes particuliers sont en effet prévus pour certaines catégories de données. C'est ainsi que si les données peuvent être qualifiées de données médicales ou sensibles, le consentement de la personne ne permettra de légitimer le traitement que s'il est écrit et peut être retiré à tout moment. À noter en outre que le Roi pourrait déterminer des cas où « l'interdiction de traiter des données sensibles relevant de l'article 6 de la LVP (les données relatives à la race, aux opinions philosophiques, religieuses, etc.) ne peut être levée par le consentement écrit de la personne concernée » (25) et que si les données sont qualifiées de données judiciaires, le consentement ne suffira pas à légitimer le traitement.

Sur les conditions du consentement

Une manifestation de volonté libre, spécifique et informée (26) est nécessaire pour légitimer le traitement. L'existence d'une **liberté** du consentement est souvent problématique car les sociétés gérant des

(24) « *Le traitement de données à caractère personnel ne peut être effectué que a) lorsque la personne concernée a indubitablement donné son consentement* », article 5, a LVP et « *par consentement de la personne concernée', on entend toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement*», article 1 §8 LVP.

(25) Article 6 §2, dernière phrase de la LVP. On peut facilement imaginer que ce soit le cas à propos de listes noires.

(26) Comme l'exige la définition même du consentement tel que repris par la LVP (voir la définition, reprise note 21).

listes noires utilisent souvent la formule du contrat d'adhésion. La Commission le souligne d'ailleurs à juste titre lorsqu'elle écrit que « l'exigence de la liberté du consentement (art. 1 § 8 de la LVP) semble problématique si ce consentement constitue la condition pour obtenir un service essentiel à la personne concernée » (27). De plus ce consentement doit être **spécifique** c'est-à-dire qu'il n'est accordé que pour une ou des finalités déterminées. Il ne pourra donc être étendu à des finalités autres que celles prévues lors de la conclusion du contrat. Quant au dernier critère qualitatif, celui du consentement **informé**, la Commission dans son avis Datassur (28) écrit que « […] la personne concernée n'a, en pratique, que rarement l'occasion de prendre connaissance des conditions générales avant de signer un contrat et que de ce fait elle n'est pas suffisamment informée ». De plus, l'article 4 de la LVP stipule que « *§ 1. Les données à caractère personnel doivent être : 2° collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables. […].* » Donc, poursuit la Commission, « *même avec le consentement de l'intéressé, le fichage n'est licite que s'il rencontre les prévisions raisonnables de l'intéressé. Par conséquent, un consentement non suffisamment informé ne suffit pas à rendre le fichage licite* ». En conclusion, ne rencontrant que très rarement les conditions imposées par la loi, le consentement doit être écarté comme cause de légitimité dans la majorité des listes noires.

II.1.3. Principe de proportionnalité : de la mise en balance de l'intérêt légitime du responsable du traitement et de l'intérêt du fiché

L'application du point f de l'article 5 LVP comme fondement de la légitimité des listes noires externes est plus délicate à traiter : « *Le traitement de données à caractère personnel ne peut être effectué*, dit cet article, que *: f) lorsqu'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le tiers auquel les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée qui peut pré-*

(27) Par exemple, « le consentement à l'utilisation des données médicales lors de la conclusion d'une assurance solde restant dû comme condition pour contracter un prêt hypothécaire ou lors de la souscription d'une assurance obligatoire RC pour les véhicules motorisés, … », Commission pour la protection de la vie privée, 15 juin 2005, avis n° 09/2005 sur un encadrement des listes noires, disponible sur http://www.moniteur.be.

(28) Commission pour la protection de la vie privée, 28 juin 2000, Avis d'initiative n° 21/2000 relatif au fichier RSR (fichier ayant pour but le signalement, entre compagnies d'assurance, des risques spéciaux en assurances incendie, accidents et risques divers) gérés par le Groupement d'intérêt économique « Datassur », disponible sur http://www.moniteur.be.

tendre à une protection au titre de la présente loi ». Les conditions de l'article peuvent être détaillées comme suit. Premièrement, le responsable du traitement doit invoquer un intérêt légitime. La notion de responsable évoque à la fois, en ce qui concerne le traitement consistant en la transmission à l'origine de l'information figurant dans la liste noire, l'entité qui transmet la donnée et participe ainsi à l'alimentation de la base de données commune et, en ce qui concerne la liste elle-même, le gestionnaire de celle-ci. En l'espèce sont souvent invoquées la gestion des risques contractuels et/ou la prévention de la fraude, autant de motifs pouvant être considérés comme légitimes tant pour la transmission des données que pour leur mutualisation (29). Que ces mêmes arguments puissent être invoqués pour justifier la transmission au tiers, à savoir l'entité ou les entités destinatrices de telles données, ne semble pas poser de questions. Deuxièmement, la finale de cet alinéa implique une mise en balance d'intérêts entre, d'une part l'intérêt légitime du responsable du traitement et d'autre part l'intérêt ou droits fondamentaux de la personne concernée.

Il est unanimement admis que si un droit ou une liberté fondamentale sont invoqués par la personne concernée, l'intérêt légitime du responsable devra être plus important que si la personne concernée invoque uniquement un intérêt légitime. « *Plus est grande la protection envisagée au bénéfice d'une catégorie, et plus sont, potentiellement, affectés les intérêts de l'autre catégorie, de telle sorte que la balance à trouver entre les intérêts des uns et des autres revêt en l'espèce un caractère primordial [...]* » (30), notait la Commission à propos d'une liste noire de locataires risquant d'être privés d'un droit fondamental consacré par la Constitution, à savoir le droit au logement consacré par l'article 23 de la Constitution. Le même raisonnement pourrait valoir pour le droit à l'éducation si des listes noires étaient établies par des institutions d'enseignement (31) et avaient pour effet de priver l'étudiant de son droit à l'enseignement.

Selon l'économie de la loi, c'est au responsable du traitement que revient la tâche de vérifier s'il dispose d'un fondement légitime lors de la création d'un traitement.

(29) Voir section I, point 2, a. p. 3.

(30) Commission pour la protection de la vie privée, 19 avril 2002, avis n° 52/2002 relatif à la constitution d'un fichier externe des locataires défaillants, p. 2, disponible sur http://www.moniteur.be.

(31) À l'inverse, à propos des listes noires mettant en cause de simples intérêts, celui d'obtenir un crédit ou une assurance, le raisonnement pourrait être différent.

II.1.4. Légitimité quant au contenu du traitement

Une attention particulière doit être accordée au principe de proportionnalité de l'article 4, 3° (32) qui implique une mise en balance entre d'une part la finalité du traitement et d'autre part les types de données collectées. La doctrine admet que cet article est une émanation du principe de proportionnalité s'appliquant à l'entièreté de la matière et non seulement à l'article 5f. Une mise en balance d'intérêts devra avoir lieu quelle que soit la légitimité du traitement et les données collectées devront se limiter au strict nécessaire à l'accomplissement de la finalité déclarée.

II.2. LE CAS PARTICULIER DES DONNÉES JUDICIAIRES

II.2.1. L'article 8, un article flou aux contours incertains

Une des questions centrales posées par l'existence des listes noires est la crainte d'une justice privée à l'égard de citoyens convaincus de non-respect d'obligations contractuelles ou pire de commissions d'infractions et qui sans autre forme de procès se verraient exclus de toute possibilité d'obtenir un bien ou un service. De telles informations ne constituent-elles pas au sens de la LVP des informations tombant sous le coup de l'article 8 et dès lors soumises au régime sévère, c'est-à-dire l'interdiction de traitement sous réserve de quelques exceptions à interpréter restrictivement.

Bien que la Commission (33) ait conscience de l'importance d'une délimitation claire de la portée de l'article 8, on peut regretter qu'elle ne profite pas de cet avis pour définir avec clarté et précision ce qu'il faut entendre par « données judiciaires » visées par l'article 8 de la loi vie privée. Cet article stipule que « *§ 1. Le traitement de données à caractère personnel* ***relatives*** *[(1)* ***à*** *des litiges* soumis *aux cours et tribunaux ainsi qu'aux juridictions administratives], [(2)* ***à*** *des suspicions, des poursuites ou des condamnations ayant trait à des* infractions*], ou [(3)* **à** *des sanctions administratives ou de mesures de sûreté] est interdit.* » Le texte vise donc trois cas distincts. D'emblée il est utile de préciser que la première catégorie s'ordonne autour du critère de

(32) « *§ 1. Les données à caractère personnel doivent être : 3° adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement.* »

(33) « *Le principe (voire la portée) de l'interdiction de traiter de telles données et les exceptions doivent être clairement définis* », Commission pour la protection de la vie privée, 15 juin 2005, avis n° 09/2005 sur un encadrement des listes noires, point 4.1.3.c, disponible sur http://www.moniteur.be

l'introduction d'une procédure devant les cours et tribunaux (34). La délimitation du champ d'application de la deuxième catégorie : « données relatives à des suspicions, des poursuites ou des condamnations ayant trait à des infractions » semble plus délicate et retiendra l'attention. Quant à la troisième, son extension est évidente et ne sera pas l'objet de commentaires de notre part.

II.2.2. Des suspicions [...] ayant trait à des infractions ?

Quel type d'informations, le législateur a t'il voulu comprendre dans la deuxième catégorie visée par l'article 8 ? Première clarification : faut-il que les suspicions, poursuites et condamnations aient trait à des infractions (1) ou la précision « ayant trait à des infractions » se limite-t-elle à la notion de condamnation (2)? Cette précision est d'importance car si le terme suspicion se rattache uniquement à la notion d'infractions, le champ de cet article se trouve considérablement réduit. En effet, prenons l'exemple d'une liste noire consistant à lister les personnes suspectées de naviguer sur internet à titre personnel plus de x heures par jour durant les heures de bureau. Si la notion de suspicion est indépendante de celle d'infraction, le traitement de ce type de données pourrait éventuellement être interdit. Par contre, si les suspicions doivent avoir trait à des infractions, le régime de droit commun sera alors applicable. Plus simplement, si les données n'ont pas trait à des infractions (suspicion de faute contractuelle, de risque d'accidents, de non-remboursement d'une créance, etc..) le régime à appliquer est celui du droit commun de la LVP.

Nous penchons pour la première interprétation. Plusieurs arguments nous confortent dans cette interprétation. *Primo*, l'argument textuel : le terme « relative » invite à analyser les différentes hypothèses énumérées auxquelles le mot « relatives » fait référence. Or cette énumération est composée de trois éléments : relatives à des litiges ; relatives [...] à des suspicions... ; relatives[...] à des sanctions administratives [...]. Si le législateur avait voulu isoler le terme « ayant trait à des infractions » aux seules condamnations, il aurait dû faire précéder « des condamnations » par la préposition « à » (35).

---

(34) Cette précision, apportée il subsiste un grand nombre d'interrogations comme le relève J. DHONT : « *À partir de quels moments les données relatives aux litiges soumis aux cours et tribunaux sont estimées être d'ordre judiciaire ? Dès la citation ou dès la comparution ? Est-ce que les instances disciplinaires sont visées par la loi ? S'agit-il obligatoirement de procédures contentieuses ? Quid des procédures gracieuses ? ...* », *op. cit.*

(35) De plus, cet argument textuel français est aussi valable en néerlandais : « *De verwerking van persoonsgegevens* ***inzake*** *geschillen voorgelegd aan hoven en rechtbanken alsook aan administratieve gerechten,* ***inzake*** *verdenkingen, vervolgingen of veroordelingen met betrekking tot misdrijven, of* ***inzake*** *administratieve sancties of veiligheidsmaatregelen, is verboden.* »

Secundo, l'argument tiré des travaux préparatoires qui précise la portée de l'article 8 « *La notion de 'suspicions, poursuites ou de condamnations relatives à des infractions' montre que l'article 8 ne s'applique pas uniquement aux condamnations pénales mais également aux données dont il ressort qu'une personne est soupçonnée ou poursuivie pour un délit* » (36). Suspicions, poursuites ou condamnations y sont vues comme un tout.

Tertio, l'argument tiré de textes internationaux : l'article 8 de la directive 46/95/CE que l'article 8 de notre loi transpose. Ce texte prévoit un régime spécifique uniquement pour les « données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ». La première catégorie vise donc l'ensemble des données relatives (ou ayant trait) à des infractions en ce compris les suspicions, poursuites ou condamnations. N'est donc interdit que ce qui a trait à des infractions et non, par exemple, une liste de personnes établies sur base de suspicions de non-rentabilité détenue par un établissement de jeux de hasard.

II.2.3. Dans un cadre judiciaire ?

Mais cette seconde catégorie vise-t-elle uniquement les suspicions, poursuites ou condamnations récoltées dans un cadre juridictionnel en l'occurrence judiciaire ? En d'autres termes, une liste de suspicions de fraudes bancaires tenue par un banquier tombe-t-elle dans le principe d'interdiction si elle n'est pas collectée dans le cadre de procédures judiciaires ? À cette dernière question nous répondons par l'affirmative. En effet, vu le postulat de rationalité du législateur, le critère distinctif de la catégorie de données judiciaires que nous analysons ne peut être identique à la première catégorie de données, celle des données relatives aux litiges soumis aux cours et tribunaux, sous peine de voir l'intérêt du deuxième alinéa fortement réduit. Si cela était le cas, cette deuxième énumération devrait être vue comme une précision de la première ce qui est contraire à l'énumération découlant du terme « relative à ».

II.2.4. Du champ de la notion d'infraction

Enfin, est-ce que l'idée des législateurs internationaux est de prévoir un régime spécifique pour ce qui a trait au champ pénal et uniquement

(36) Voy. Projet de loi transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, *Doc.parl.*, Ch. repr., sess. ord. 1997-1998, n°1566/1 du 20 mai 1998, p.42. Également disponible sur www.lachambre.be, session 49.

à celui-ci ? Une analyse des textes qui ont précédé la loi de 1992 revue en 1998 et dont notre loi s'inspire permet de répondre à cette question. L'article 6 de la Convention n° 108 du Conseil de l'Europe (37) et les considérants de ce texte poussent à répondre par l'affirmative. La directive quant à elle énumère trois cas qui amènent à penser que le fait permettrait d'avoir énuméré distinctement les infractions et les condamnations pénales aux États membres d'appliquer ce régime d'exception à des infractions non pénales. Sans doute cette référence aux textes dont la loi belge s'est inspirée ne suffit point dans la mesure où la convention du Conseil de l'Europe et la directive ne prévoient qu'un minimum de garanties et que les États membres restent libres de prévoir un niveau de protection plus élevé (38).

Était-ce l'intention du législateur belge lors de la modification de la loi en 1998 d'inclure dans les données judiciaires visées par l'article 8, les informations relatives à des infractions non pénales ? Les travaux préparatoires de cette législation indiquent que *« la notion de 'suspicions', poursuites ou de condamnations relatives à des infractions montre que l'article 8 ne s'applique pas uniquement aux condamnations pénales mais également aux données dont il ressort qu'une personne est soupçonnée ou poursuivie pour un délit »* (39). Il faut souligner que le terme employé est celui de « délit ». Les infractions non pénales et les contraventions ne seraient pas visées par cet article ; seules les données relatives à des délits et des crimes sont donc à considérer comme données judiciaires au sens de l'article 8. De plus, le législateur a, semble-t-il, voulu étendre la notion de données judiciaires au delà des condamnations pénales mais à aucun moment n'a envisagé de l'étendre à des infractions non pénales. La notion « d'infraction » renverrait donc au champ pénal exclusivement et non au non-respect d'obligations civiles.

(37) Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Conseil de l'Europe, signée à Strasbourg le 28 janvier 1981. Ce texte prévoit un régime particulier pour des « Catégories particulières de données ». Il vise, entre autres, les « données à caractère personnel concernant des condamnations pénales » et uniquement celles-là. Le rapport explicatif en son point 47 va d'ailleurs dans le même sens : « Par «condamnations pénales » il y a lieu d'entendre : des condamnations fondées sur une loi pénale et dans le cadre d'une procédure pénale ».

(38) La directive 95/46/CE va même plus loin et prévoit expressément cette possibilité pour les législateurs nationaux.

(39) Voy. Projet de loi transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, *Doc.parl.*, Ch. repr., sess. ord. 1997-1998, n°1566/1 du 20 mai 1998, p.42. Egalement disponible sur www.lachambre.be, session 49.

Afin d'être complet sur la notion de données judiciaires et la légitimité de leur utilisation, l'arrêt du Conseil constitutionnel français (40) doit être mentionné. L'article 9 de la loi française prévoit que « *Les traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté ne peuvent être mis en place que par : […] 3° Les personnes morales victimes d'infractions ou agissant pour le compte desdites victimes pour les stricts besoins de la prévention et de la lutte contre la fraude ainsi que de la réparation du préjudice subi, dans les conditions prévues par la loi ; […]* ». C'est précisément l'hypothèse de la création de liste noire qui est visée par cet article. Le Conseil constitutionnel français déclara cet article « entaché d'incompétence négative » pour deux raisons, l'une parce qu'elle contenait une délégation de pouvoirs inconstitutionnelle et l'autre parce que la définition donnée par l'article est ambiguë. Le caractère inconstitutionnel de la délégation de pouvoir que la loi réalise au profil de la CNIL, l'équivalent de notre CPVP, sera examiné plus loin. Par contre, le second motif de rejet par le Conseil constitutionnel mérite l'attention. Sur l'ambiguïté de la notion de « prévention et de lutte contre la fraude », le Conseil s'exprime comme suit : la disposition « *est ambiguë quant aux infractions auxquelles s'applique le terme de fraude ; elle laisse indéterminée la question de savoir dans quelles mesures les données traitées pourraient être partagées ou cédées, ou encore si pourraient y figurer des personnes sur lesquelles pèse la simple crainte qu'elles soient capables de commettre une infraction ; qu'elle ne dit rien sur les limites susceptibles d'être assignées à la conservation des mentions relatives aux infractions* ».

L'arrêt français mérite qu'on s'y arrête au moment où est envisagée une législation des listes noires dans notre pays. Le Conseil réclame une définition légale précise des données couvertes chez nous par l'article 8, en particulier cette catégorie vise-t-elle des informations sur la crainte de commissions d'infractions conservées par des entités privées et en dehors de tout contentieux judiciaire proprement dit ? Par ailleurs, en cas de réponse positive à la première question, le Conseil exige que des garanties soient introduites par la loi sur la durée de conservation et les conditions de partage et cessions de telles données. Ces exigences nous semblent répondre aux exigences d'une loi « prévisible et proportionnée », exigences déduites du libellé même de l'article 8.2 de la CEDH par la jurisprudence de la Cour de Strasbourg. Ces

(40) Décision n° 2004-499 DC, *Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi No 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, 29 juillet 2004, *Recueil*, p. 126 ; *Journal officiel*, 7 août 2004, p. 14087. [*Non conformité partielle*] disponible sur http://www.conseil-constitutionnel/fr/decision/2004/2004499/index.htm.

mêmes exigences sont requises par la Cour d'arbitrage belge et dès lors il faudra en tenir compte sous peine de voir la législation qui pourrait être proposée en Belgique encourir les mêmes critiques que celles adressées à la loi française.

II.2.5. Des causes de légitimé particulières aux données judiciaires

En résumé, on peut donc distinguer trois cas de données dont le traitement sera en principe interdit. Le premier vise toute donnée relative à des litiges *soumis* (41) aux cours et tribunaux aussi bien civils que pénaux. Les données concernées sont uniquement celles qui peuvent être collectées à partir du moment où un litige est effectivement introduit. Le deuxième est plus large et vise à la fois les suspicions, poursuites et condamnations, *dans un cadre judiciaire ou non* mais uniquement *pour ce qui a trait à un délit ou crime*. Le troisième vise les sanctions administratives ou mesures de sûreté et n'appelle pas de commentaires particuliers.

Cependant, lorsqu'on est face à de telles données, le traitement reste possible si une des cinq hypothèses prévues par la loi est remplie. Comme annoncé plus haut, l'une d'entre elles va plus particulièrement retenir notre attention : la gestion de son propre contentieux (42). Mais que recouvre réellement cette notion ? Ce sont les données nécessaires pour intenter une procédure pénale, civile, administrative ou en vue d'une mesure de sûreté, ou celles qui constatent ces mêmes sanctions et condamnations. Nous pouvons citer en ce sens la Commission elle-même, qui dans son avis IFPI arrive à la conclusion que les conditions prévues par la LVP *« permettent donc à une maison de disques, à l'IFPI ou à la SABAM de traiter des données relatives à une infraction précise qu'elles ont pu constater,* ***dans la mesure où elles se situent dans une phase au moins préparatoire à un litige*** ». Comme toute exception celle-ci doit s'interpréter restrictivement. Par conséquent, la récolte de telles informations en dehors de toute préparation à une action en justice afin de constituer une liste noire ne trouve pas justification aux yeux de la LVP.

(41) Le terme « soumis » implique qu'une procédure soit effectivement entamée devant les cours et tribunaux.

(42) Le texte stipule que *« § 2. L'interdiction de traiter les données à caractère personnel visées au § 1er n'est pas applicable aux traitements effectués : c) par des personnes physiques ou par des personnes morales de droit public ou de droit privé pour autant que la gestion de leurs propres contentieux l'exige ».*

II.3. DES DROITS DE LA PERSONNE CONCERNÉE ET DES OBLIGATIONS CORRÉLATIVES DU RESPONSABLE DU TRAITEMENT

II.3.1. Droit d'information

Le régime légal prévu par la LVP repose sur le principe de transparence. Les personnes fichées doivent être informées, sauf rares exceptions, de ce fichage, du type d'informations collectées, du responsable du traitement, du partage du fichier, etc..(43). Le droit à l'information constitue donc la pierre angulaire de la LVP et permet l'exercice effectif des autres droits subjectifs qui lui sont reconnus par la loi. Cette obligation d'information, sans d'ailleurs préciser les modalités de celle-ci, impose une information sur les possibilités d'être inscrit sur les listes noires au moment de la conclusion du contrat. Il est cependant dommage que cette information n'ait lieu que dans une phase préalable et soit souvent bien éloignée de l'éventuel inscription sur la liste noire. De plus, actuellement, il est fort difficile pour un citoyen de gérer efficacement l'ensemble des données traitées avec pour corollaire le risque d'être dans l'impossibilité d'exercer son droit d'accès ou de contestation.

II.3.2. Droit d'accès et de rectification

La LVP prévoit la possibilité pour le fiché d'accéder aux données contenues dans la base de données et de les rectifier si celles-ci sont erronées. Ce droit devrait être renforcé pour éviter les conséquences catastrophiques liées à l'empêchement de souscrire à certains services considérés comme essentiels.

II.3.3. Les systèmes de décisions automatisées

L'interdiction des traitements fondant une décision purement automatisée est prévue par l'article 12 *bis* LVP (44). Elle est liée à la condition que la décision ainsi prise affecte de manière significative la personne ou ait des effets juridiques envers elle. Dans la grande majorité des cas, les listes noires seront comprises dans cette interdiction. Certes, le législateur peut autoriser ce traitement dans certains cas. Il

(43) Voy. article 9 de la LVP, *op.cit.*

(44) « *Une décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité. L'interdiction prévue à l'alinéa 1^er^ ne s'applique pas lorsque la décision est prise dans le cadre d'un contrat ou est fondée sur une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance. Ce contrat ou cette disposition doivent contenir des mesures appropriées, garantissant la sauvegarde des intérêts légitimes de l'intéressé. Il devra au moins être permis à celui-ci de faire valoir utilement son point de vue », article 12 LVP.*

lui revient d'opérer la balance d'intérêt protection vie privée – intérêt légitime du traitement automatisé. Par contre, il nous semble qu'autoriser ce traitement sur base d'un contrat est plus délicat bien que l'obligation dans ce cas de prévoir des garanties (par exemple, le droit à un entretien) est prévue par la loi. Premièrement, les même remarques que pour le consentement valent ici. Deuxièmement, comment justifier la liberté de la personne de contracter pour des services considérés comme essentiels ou découlant de droits fondamentaux ?

Au delà, même si la consultation d'une liste noire n'entraîne pas une prise de décision automatique, on conçoit que la personne qui doit prendre la décision d'accepter ou non un client repris sur la liste marque quelque hésitation et l'acceptation d'un tel client entraînera sans doute sa responsabilité s'il s'avère que le client malgré tout accepté s'avère par la suite un mauvais client. Bref, il serait sans doute utile que la personne concernée du moins dans le cadre de listes externes (45) soit avertie lorsqu'elle entre en contact avec une entreprise qui utilise ce type de liste, que celle-ci prendra, outre les informations collectées auprès du candidat client, des informations (46) auprès du responsable qui tient la liste noire.

II.3.4. Principe de sécurité : des obligations existantes ... mais peu respectées

Le principe de sécurité permet d'assurer à la fois l'intégrité des données et leur confidentialité par la mise en place de mesures organisationnelles (Qui peut décider de déposer une information ? Qui peut la lire ? Auprès de qui une contestation sur une donnée pourra t'elle avoir lieu ?,etc.) et techniques (mot de passe, encryptage de certaines communications, conservations des log-in et log-out des bases de données, etc.)). De plus, une obligation de diligence est prévue concernant la mise à jour et l'exactitude des données. Sans entrer dans les détails il faut rappeler que cette disposition liste une série d'obligations permettant de rencontrer nombre de craintes concernant la sécurité, craintes formulées à l'encontre des listes noires (47) encore faut-il qu'elles soient respectées ce qui n'est pas le cas dans tous les traitements que constituent les listes noires.

---

(45) En cas d'utilisation de listes noires internes, on peut facilement concevoir que la personne déjà en relations d'affaires avec le responsable du traitement s'attende raisonnablement à ce que son contractant utilise des informations sur le passé contractuel du client et ses agissements.

(46) À noter que l'article 9 sur le devoir d'information de celui qui collecte des données auprès de la personne concernée n'oblige pas à délivrer ce type d'information.

(47) Sur ces craintes, *supra* I.2.2.

III. FAUT-IL LÉGIFÉRER EN LA MATIÈRE ?

III.1. LES FONDEMENTS POSSIBLES D'UNE INTERVENTION LÉGISLATIVE

Sans nous prononcer à ce stade sur l'opportunité d'une intervention législative et son contenu, relevons les arguments sur lesquels pourrait s'appuyer une telle intervention.

Un premier argument est tiré de l'obligation positive (48) mise à charge des États par l'article 8 de la Convention européenne des droits de l'homme de garantir la protection de la vie privée et familiale (49). Cette obligation se dégage d'une jurisprudence abondante de la Cour européenne de Strasbourg. L'article 22 de notre Constitution relaie cette obligation positive lorsqu'il stipule que « *La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit.* ». Comme le notent Vande Lanotte et Haeck (50), c'est le devoir de l'État d'intervenir lorsqu'un droit fondamental est mis en cause par des pratiques privées ou administratives. Dans la mesure où les listes noires remettent en cause certains droits fondamentaux tels par exemple, le droit au logement, le droit à l'emploi ou la liberté de circulation, l'intervention de l'État se justifie. On notera qu'un tel fondement ne justifie l'intervention réglementaire de l'État que dans une mesure très limitée et que la nécessité de démontrer l'atteinte à un droit fondamental peut ne pas être évidente. Ainsi, peut-on considérer que la liste noire qui pourrait priver un citoyen d'une possibilité de s'assurer met en cause un droit fondamental, rien n'est moins sûr sauf à inter-

---

(48) F. SUDRE (ed.), *Le droit au respect de la vie privée au sens de la CEDH*, Nemesis / Bruylant , 2005, p.27.

(49) Nombre d'auteurs (Voir les nombreuses références citées par P. DE HERT et S. GUTWIRTH, « Controletechnieken op de werkplaats : herbeschouwingen in het licht van persoons gegevens beschermingsrecht », *Orientatie*, 1993, n° 5, 125 et s. et J. VAN DE LANOTTE et Y. HAECK, *op.cit.*, pp. 186 et s. ; voir également Cass. 27 fév. 2001, *Vigiles*, 2001, pp. 153 et s., note P. DE HERT, à propos du placement d'une caméra vidéo dans un grand magasin où la Cour fait référence à l'article 22 de la Constitution et semble donc accepter implicitement son effet horizontal) soutiennent également qu'en droit interne du moins, l'article 8 a un effet horizontal, c'est-à-dire que le prescrit vaut aussi bien dans les relations entre particuliers et administrations qu'entre particuliers. L'avis annoté mentionne également l'effet horizontal de l'article 22 comme fondement de l'intervention du législateur.

(50) J. VANDE LANOTTE, Y. HAECK, *Het Europees verdrag to bescherming van de rechten van de mens in Hoofdlijnen*, Antwerpen, Maklu, 1997, Part. I, p. 186 à 196. Voir aussi, l'attendu de la Cour de Strasbourg : « *...à cet engagement plutôt négatif peuvent s'ajouter des obligations positives inhérentes à un respect effectif de la vie familiale* » (Cour eur. D.H., 3juin 1979, *Marckx c. Belgique*, Req. 6833/74, § 31). Sur ces obligations positives et l'analyse des décisions strasbourgeoises, lire H. VUYE, « Over vliegtuigen, luchthavens, lawaaihinder, milieuhinder en mensenrecten...Welke rechtsbescherming bieden artikel 8 EVRM en artikel 22 Grondwet », *R.G.D.C.*, 2003, p. 490 . Cf. également L. BYGRAEVE, « Data Protection Pursuant to the Right to Privacy in Human Rights Treaties », 2003, *Int. J.L. and Inf. Tech.*, 6, n° 3, p. 25

préter largement la notion de dignité humaine consacrée par l'article 23 de la Constitution.

Un autre fondement de l'intervention apparaît possible : l'article 20 de la directive stipule que « 1. Les États membres précisent les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées et veillent à ce que ces traitements soient examinés avant leur mise en oeuvre. 2. De tels examens préalables sont effectués par l'autorité de contrôle après réception de la notification du responsable du traitement ou par le détaché à la protection des données, qui, en cas de doute, doit consulter l'autorité de contrôle. 3. Les États membres peuvent aussi procéder à un tel examen dans le cadre de l'élaboration soit d'une mesure du Parlement national, soit d'une mesure fondée sur une telle mesure législative, qui définisse la nature du traitement et fixe des garanties appropriées». Il est à souligner que l'écriture de cette disposition visait précisément des traitements comme les listes noires comme cela ressort du considérant 53 : « Considérant que, cependant, certains traitements sont susceptibles de présenter des **risques particuliers au regard des droits et des libertés des personnes concernées**, du fait de leur nature, de leur portée ou de leurs finalités **telles que celle d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat**, ou du fait de l'usage particulier d'une technologie nouvelle ; qu'il appartient aux États membres, s'ils le souhaitent, de préciser dans leur législation de tels risques ». On notera que l'approche hollandaise nous apparaît suivre l'approche préconisée par l'article 20 de la directive. La loi de 1992 (51) ne fait écho à cette disposition pourtant centrale que de manière partielle, par l'article 17*bis*, en renvoyant au Roi le soin d'établir des garanties supplémentaires pour les traitements présentant des risques particuliers. A l'heure actuelle, aucune mesure n'a encore été prise.

Un troisième argument pourrait plaider en faveur de l'intervention législative. Il s'inscrit à la suite de nos réflexions sur l'ambiguïté de la notion de données « juridictionnelles », visée à l'article 8 de notre loi de 1992. Sans doute, avons nous cherché à démontrer que la notion de « suspicion d'infractions » ne devait pas s'étendre des informations quant au non-respect établi ou supposé de dispositions non pénales mais il n'empêche que cette disposition devrait viser, au delà des seules suspicions d'infractions pénales, certaines données détenues par les

(51) Plus étonnant encore, le document de travail du Groupe européen de protection des données dit de l'article 29, adopté le 3 octobre 2002, ne fait pas allusion à cet article même si dans ses conclusions il attire l'attention sur le fait qu'il existe des risques particuliers à propos de listes concernant un grand nombre de citoyens dans des secteurs d'importance majeure (les télécommunications et le secteur financier).

responsables de traitement dans la mesure où on peut à la suite de la Commission considérer qu'elle présente « *un caractère plus dommageable et plus délicat encore, dans la mesure où elles n'ont pas été soumises à l'examen du juge ni à une quelconque procédure contradictoire* » (52). De plus, les limites fixées par la loi de 1992 au traitement des données judiciaires sont telles que leur traitement ne peut s'opérer pour un responsable de traitement privé que dans le cadre de la seule gestion de leur propre contentieux. De telles limites sont, nous semble-t-il, trop étroites dans la mesure où les entreprises doivent légitimement pouvoir, seules voire conjointement, prévenir la commission d'infractions dont elles seront les premières victimes. Que la loi nouvelle sur les listes noires soit l'occasion de modifier sur ce point la loi de 1992 à la fois en légitimant mais surtout en entourant le traitement de ces données juridictionnelles de sévères garanties peut également être avancé comme argument. On soulignera à nouveau, que c'est à propos de ce point précis que le projet de loi français (53) a été attaqué devant le Conseil constitutionnel français et que, comme le relate l'avis de la Commission annoté, *« les traitements destinés à lutter contre la fraude requerront* (54) *en France une disposition ad hoc, avec les garanties appropriées et spécifiques répondant aux exigences de la Constitution (française)* ». Les critiques adressées par le Conseil constitutionnel français méritent qu'on s'y attarde.

III.2. QUEL CONTENU ?

L'avis du Groupe dit de l'article 29 analyse de manière systématique l'application de la directive aux listes noires, l'avis de la Commission belge le fait également à propos de la loi de 1992. Il est patent que ces dispositions européennes et nationales bien appliquées pourraient résoudre nombre de problèmes rencontrés comme nous le remarquions d'emblée. Ainsi le principe de qualité des données oblige à limiter le traitement à des données adéquates, à ne pas les conserver au delà d'une certaine durée. Le principe de transparence exige de veiller à l'information des personnes concernées tant de l'existence du fichier « liste noire » que de sa communication lorsqu'elle est externe à

(52) Commission pour la protection de la vie privée, 15 juin 2005, avis n°09/2005 sur un encadrement des listes noires, point 4.1.3.c, disponible sur http://www.moniteur.be .

(53) L'article 9 de la loi française prévoyait que « *Les traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté ne peuvent être mis en place que par : [...] 3° Les personnes morales victimes d'infractions ou agissant pour le compte desdites victimes pour les stricts besoins de la prévention et de la lutte contre la fraude ainsi que de la réparation du préjudice subi, dans les conditions prévues par la loi ; [...]* ». C'est précisément l'hypothèse de la création de liste noire qui était visée par cet article

(54) Cette disposition n'a pas encore été prise.

l'entreprise. Le principe de sécurité veille à assurer au delà de l'intégrité des données, leur confidentialité et plaide pour des mesures organisationnelles. Un simple rappel de ces règles et l'exercice par la Commission de ses pouvoirs d'enquête et, le cas échéant, de dénonciation aux parquets peuvent-ils dès lors suffire ?

La particularité des listes noires qui constituent un outil de décision vis-à-vis des personnes concernées, qu'elles soient internes ou externes, justifie sans doute des précautions supplémentaires que la Commission peut encadrer elle-même. L'exemple hollandais (55) d'un vade mecum expliquant la signification précise des diverses dispositions de la loi appliquées aux listes noires est sans doute utile. Au delà, la mise à disposition d'un questionnaire contenant une check list spécifique (56) à remplir par les responsables de tels traitements et à notifier à

(55)Voir le site : http://www.cbpwet.nl/themadossiers/th_zwl_melden.stm.

(56) La « **Checklist Zwarte Lijsten** » est présentée comme suit :De checklist'*Zwarte lijsten*'biedt een eerste handreiking om een zwarte lijst zo zorgvuldig mogelijk in te richten. De checklist biedt toetsingsvragen die beantwoord dienen te worden om te kunnen voldoen aan de normen van de Wet bescherming persoonsgegevens.

- Wat is het doel van de zwarte lijst?
- Welke motieven maken de aanleg van de lijst noodzakelijk?
- Welke criteria gelden voor plaatsing op een zwarte lijst, dus welke gedragingen komen daarvoor in aanmerking?
- Hoe verifieert de verantwoordelijke of de gegevens juist en nauwkeurig zijn?
- In hoeverre wordt de toegang voor de betrokkene voor bepaalde voorzieningen afgesneden en welke alternatieven resteren?
- Hoe essentieel is de voorziening voor de betrokkene?
- In hoeverre is het doel van de lijst te kwalificeren als een'bedrijfs(tak)belang'?
- In hoeverre weegt het belang van het bedrijf of de bedrijfstak op tegen de schade die een betrokkene oploopt als hij of zij op een zwarte lijst wordt geplaatst (proportionaliteit)?
- Kan het doel niet langs andere weg bereikt worden (subsidiariteit)?
- Onderzoekt de verantwoordelijke de reden van opname als de betrokkene, met wie hij een contractuele relatie wil aangaan, op een zwarte lijst voorkomt?
- Op welke wijze en van wie worden de persoonsgegevens verkregen?
- Welke waarborgen zijn er om te voorkomen dat niet meer gegevens worden verwerkt dan noodzakelijk?
- Worden de persoonsgegevens verstrekt aan derde partijen?
- Welke (organisatorische en technische) maatregelen heeft de verantwoordelijke getroffen om de persoonsgegevens op de zwarte lijst te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking?
- Hoe en op welk moment wordt de betrokkene meegedeeld dat, en met welke reden, hij of zij op een zwarte lijst is geplaatst?
- Wordt de reden van contractsweigering aan de betrokkene meegedeeld en op welke wijze?
- Hoe kan de betrokkene zijn inzage- en correctierecht uitoefenen?
- In welke gevallen wordt de betrokkene van de lijst verwijderd?
- Hoe lang blijven de persoonsgegevens op de lijst staan?

l'autorité de protection de même que la confection d'un modèle de clause d'information des personnes concernées sur l'existence des listes noires sont prévues par l'autorité néerlandaise de protection et sont sans doute utiles à introduire chez nous également. Faut-il aller plus loin ?

Sans doute, n'est-ce pas aux auteurs d'un article de doctrine de trancher dans un débat qui justifie un débat démocratique mais simplement de soumettre à ce débat quelques réflexions en ce domaine.

La loi actuelle présente face aux traitements que constituent les listes noires dites « externes » quelques lacunes pour permettre d'atteindre l'objectif de protection des données souhaité. La première concerne le devoir d'information lorsque communication d'une donnée est adressée au responsable de la liste noire externe. Sur ce point, la loi actuelle (57) n'oblige pas ce dernier à une information directe de la personne concernée. Il s'agirait d'obliger le responsable de la liste de prévenir la personne concernée de son enregistrement, comme c'est le cas pour la liste négative des débiteurs défaillants, liste tenue par la Banque nationale. À cela, pourrait s'ajouter une information d'office sur la consultation de listes noires externes avant d'accorder ou non un service ou la vente d'un bien (décision d'octroi de prêt ou de refus, par exemple), en l'espèce les listes noires (58). Autre point, la question de l'interdiction de listes noires trans- ou multi-sectorielles même si sans doute le principe de finalité déterminée et spécifique peut suffire à ce propos. Il est difficile d'admettre qu'un même responsable croise des listes provenant de différents secteurs. La publication de listes noires par tous moyens y compris les médias électroniques même dans le cadre de la presse pourrait être interdite. Enfin, pour des listes propres à un secteur comme Préventel ou Datassur, l'existence d'un service « indépendant » chargé de la réception des plaintes et de leur suivi apparaît nécessaire (59) tant les conséquences d'un fichage erroné, incom-

---

• Is er een protocol waarin het beleid met betrekking tot de zwarte lijst is vastgelegd?

(57) Cf. *supra* nos réflexions à propos des termes « sauf si la personne en est déjà informée », utilisés à l'article 9 § 2 qui pourraient permettre de considérer l'information donnée in *illo tempore* lors de la signature du contrat par le premier responsable avec la personne concernée, information sur une possibilité de transfert comme suffisante dans le chef du responsable ultérieur. À noter que le règlement Datassur prévoit la notification par Datassur d'une information sur son enregistrement propre.

(58) À noter que cette information pourrait se faire à deux moments du processus. Premièrement, au moment de la communication des données. Il s'agirait alors de prévenir la personne que les décisions la concernant peuvent être prises sur base d'une consultation de listes noires. Une autre solution serait d'inclure cette information dans la décision (éventuellement sous la forme d'une motivation).

(59) À cet égard on peut songer que cette fonction soit confiée au « préposé à la protection des données » dont l'existence est prévue à l'article 17 bis de la loi de 1992 sur le modèle allemand et encouragé par l'Union européenne. Cet article prône la création de « préposés à la protection des

plet ou de données obsolètes sont importantes (60). On pourrait, comme certains pays l'envisagent, sanctionner par des dommages et intérêts forfaitaires chaque consultation de listes noires non conforme aux prescrits de la loi, ce qui, d'une part, faciliterait le recours des personnes reprises sur de telles listes et, d'autre part, amènerait les responsables de telles listes à se mettre en conformité à la loi.

Reste la question des traitements de données relatives à des infractions présumées, constatées ou jugées pour lesquels la loi hollandaise prévoit un régime spécial (61) et que la loi française envisageait de réglementer (62). Le flou actuel dénoncé (*supra*) et l'impraticabilité des solutions extensives données au champ d'application de la loi de l'article 8 de la loi de 1992 qui condamne des traitements nécessaires pour une entreprise ou pour un secteur qui désire loyalement lutter contre la criminalité amènent le rejet de ces solutions dans la pratique. Bref, il faut clarifier et une réglementation est utile sur ce point. Une telle réglementation autoriserait certes explicitement le traitement de ces données par des entreprises privées ou des associations d'entreprises privées et ce au delà de la gestion de leur propre contentieux mais, dans le même temps, les soumettrait à de sévères conditions. Elle devrait notamment répondre à certaines qualités telles que celles dictées par l'article 8.2 de la Convention européenne des droits de l'homme et la jurisprudence qui en a suivi. On rappelle ainsi qu'« *Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est* prévue par la loi *et qu'elle constitue une mesure qui, dans une société démocratique, est* nécessaire *à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.* ».

Cette réglementation doit être le fait de la loi. Il s'agit, première raison, de modifier la loi de 1992 et seule une loi peut le faire. Une autre

---

données » nommés par le responsable du traitement et « chargés d'assurer, d'une manière indépendante, l'application de la présente loi ainsi que de ses mesures d'exécution ». Un arrêté royal devait être pris à cet égard. On regrettera sur ce point le silence du Roi.

(60) On pourrait considérer que cette obligation se déduise de l'article 16 de la loi de 92 qui prescrit l'obligation de prendre des mesures de sécurité adéquates aux risques encourus par les personnes concernées du fait de leur traitement.

(61) ...c'est la procédure dite du » voorafgaand onderzoek » , c'est-à-dire de l'examen préalable par l'autorité néerlandaise de protection des données prévue sur base de l'article 20 de la directive dans trois cas seulement : utilisation de numéros d'identification personnels pour des communications au delà des finalités de départ ; collecte de données sans information préalable et communications de données pénales ou de données relatives à des comportements illicites ou répréhensibles . Ce dernier cas est celui visé des listes noires de données relatives à des infractions.

(62) Il est à noter que dans ces deux pays aucune réglementation des listes noires n'est envisagée au delà de ces listes relatives à des infractions pénales.

raison est l'interprétation restrictive donnée à l'article 22 de la Constitution belge. Si en effet, l'article 8 CEDH n'exige pas une loi au sens formel, par contre, au niveau belge, le Conseil d'État et la Cour d'arbitrage ont précisé que le terme loi renvoyait bien à la loi au sens strict, d'acte du législatif. Le Conseil d'État, dans un avis déjà ancien (63) mais de manière constante depuis, détermine la répartition des compétences entre législatif et exécutif comme suit : « *l'article 22 de la Constitution impose en particulier au législateur fédéral l'obligation de garantir la protection du droit au respect de la vie privée et familiale ; il est, à l'inverse, seul habilité à déterminer les cas et les conditions dans lesquels ce droit peut souffrir certaines restrictions* (64)». La Cour d'arbitrage dans un arrêt du 21 décembre 2004 (65) écrit que « *Bien que, en utilisant le terme « loi », l'article 8.2 de la Convention européenne précitée n'exige pas que l'ingérence qu'il permet soit prévue par une « loi », au sens formel du terme, le même mot « loi » utilisé à l'article 22 de la Constitution désigne une disposition législative. Cette exigence constitutionnelle s'impose au législateur belge, en vertu de l'article 53 de la Convention européenne, selon lequel les dispositions de la Convention ne peuvent être interprétées comme limitant ou portant atteinte aux droits de l'homme et aux libertés fondamentales reconnues notamment par le droit interne* ».

Comment envisager le contenu de cette loi : faut-il déléguer à la Commission le soin de fixer dans le cadre d'une autorisation les conditions de tels traitements ? Une telle délégation pose des problèmes constitutionnels au regard de nos principes constitutionnels fixés par l'article 33 (66) et fait de la Commission de protection de la vie privée une autorité administrative soumise au contrôle du Conseil d'État du moins en ce qui concerne ce type d'intervention (67). La pratique hollandaise directement inspirée de l'article 20 de la directive

(63) Avis du Conseil d'État : projet de loi organique des services de renseignement et de sécurité, *Doc. parl.* Ch., 1995-96, n°638/1, p.31

(64) Voy également J. VELAERS, « De Grondwet en de Raad van State, afdeling wetgeving. Vijftig jaar adviezen aan wetgevende vergaderingen », in *Het licht van de rechtspraak van het Arbitragehof*, Anvers, Maklu, 1999, p.154

(65) C.A., 21 décembre 2004, Recours en annulation n° 202/2004 de la loi du 6 janvier 2003 concernant les méthodes particulières de recherche et quelques autres méthodes d'enquête, introduit par l'a.s.b.l Ligue des droits de l'homme et autres, disponible sur http://www.arbitrage.be.

(66) À noter également en ce sens, les remarques du Conseil constitutionnel français dans la décision déjà mentionnée

(67) En effet, la Commission, dans la mesure de l'exercice de ses pouvoirs de décision constitue une « autorité administrative » « *dans la mesure où leur fonctionnement est déterminé et contrôlé par les pouvoirs publics et qu'elle peut prendre des décisions obligatoires à l'égard des tiers...* » (Sur ces critères, lire D. DE ROY, « Être ou ne pas être ...autorité administrative », *Droit communal*, 2002/2, pp. 200 et s. et F. VANDENDRIESSSCHE, « De invulling van het begrip administratieve overheid na de arresten Gimvindus en BATC van het Hof van Cassatie », *R.W.*, 2000, pp. 497 et s..

95/46/CE (68) prévoit une procédure peut-être plus complexe mais plus respectueuse de nos principes constitutionnels et démocratiques. Il s'agit de contraindre les responsables de tels traitements à passer par une procédure d'examen préalable par l'autorité de contrôle, en l'occurrence la Commission de protection de la vie privée. Celle-ci instruit le dossier et se charge, en cas de doute, de consulter les représentants des groupes intéressés. En cas de décision négative quant à un tel projet de traitement, le responsable qui a introduit le dossier peut recourir au Ministre de la Justice pour faire annuler la décision de l'autorité. Cette procédure ouverte et de dialogue laisse en outre la dernière décision au politique.

Faut-il élargir le régime qui serait prévu pour ces listes particulières de lutte contre la fraude à d'autres listes (69), ainsi à des listes de simples mauvais payeurs qui pourraient, étant donné l'étendue du marché couvert par la liste et le domaine concerné, se voir privés d'un service ou d'un droit essentiel dans nos sociétés pour assurer la dignité humaine ou qui se verraient priver d'un droit fondamental. On sait que l'État dispose de différents moyens pour obtenir la garantie du respect de tels droits, ainsi le droit à un service universel ou à un minimum de moyens d'existence. Ainsi, les droits à des services bancaires , téléphoniques ou d'électricité dits minima ou universels, le droit à une couverture d'assurance vis-à-vis de certains risques ont été proclamés sur base d'instruments parfois autres que réglementaires.

Une discussion sur les questions de l'interdiction ou non de listes noires dans certains secteurs ou sur la nécessité d'une réglementation spécifique à une liste noire sectorielle se pose donc dans un contexte de discussions politiques délicates : qui supporte les risques liés aux problèmes de débiteur défaillant, le fournisseur de biens et services, la collectivité des fournisseurs et/ou l'État ? L'État doit-il s'octroyer le monopole de la mise sur pied d'une liste noire vu le bien ou service envisagé ? La constatation de tels enjeux plaide pour une décision finale par les autorités constitutionnellement en charge des choix politiques, le législateur. On note que le législateur en matière de crédit à la consommation n'a pas hésité à intervenir pour encadrer les listes noires et créer sous son contrôle une liste gérée par la Banque nationale, liste dont les modalités de fonctionnement sont précisées par une loi. On peut imaginer qu'il intervienne à d'autres propos lorsqu'il s'agira de garantir l'accès à un service nécessaire à la dignité humaine ou à

(68) En particulier le point 2 de l'article 20 cité *supra*.

(69) On note que la CNIL dans son dossier sur les listes noires limite la réglementation envisagée à ces seules listes. Voir Commission Nationale de l'Informatique et des Libertés (CNIL), Rapport sur les listes noires, *Documentation française*, novembre 2003, p.5, disponible sur http://lesrapports.ladocumentationfrancaise.fr .

l'exercice d'un droit fondamental. Faut-il dans ce contexte dénier tout rôle à la Commission de protection de la vie privée ? N'est-ce pas son rôle (70), dans le cadre des notifications qu'elle reçoit quant à la création de listes noires tant dans le secteur public que privé, d'intervenir d'initiative (71) lorsqu'il appert que le traitement est « susceptible de présenter des risques particuliers au regard des droits et libertés des personnes concernées » ? Le récent rattachement de la Commission au Parlement par la loi du 26 février 2003 (72) favorise ce dialogue entre législatif et l'autorité de protection des données et augure du bon suivi de telles initiatives si elles étaient prises.

(70) D'ailleurs, le considérant 54 de la directive 95/46 sur la protection des données personnelles vise cette situation et suggère aux États membres cet examen préalable : « *considérant que, au regard de tous les traitements mis en oeuvre dans la société, le nombre de ceux présentant de tels risques particuliers devrait être très restreint ; que les États membres* ***doivent prévoir, pour ces traitements, un examen préalable à leur mise en oeuvre****, effectué par l'autorité de contrôle ou par le détaché à la protection des données en coopération avec celle-ci; que, à la suite de cet examen préalable, l'autorité de contrôle peut, selon le droit national dont elle relève, émettre un avis ou autoriser le traitement des données ; […]* ».

(71) Comparer avec ce passage de l'avis de la Commission (Avis, point 4.3.1 a)). « Au moment d'évaluer l'exigence de nécessité sociale, l'autorité devra, notamment, veiller au caractère des services pour lesquels la liste noire serait instaurée et examiner dans quelle mesure la liste noire pourrait répondre à une nécessité sociale. Ainsi, il serait pertinent de vérifier si la liste noire compromet ou est susceptible de compromettre l'accès à des services essentiels et/ou des droits et libertés constitutionnels du citoyen ».

(72) Loi du 26 février 2003 modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale en vue d'aménager le statut et d'étendre les compétences de la Commission de la protection de la vie privée, *M.B.*, 26 juin 2003, p. 34416. L'article 2 de cette loi modifie l'article 23 de la loi du 8 décembre 1992 et stipule : « Il est institué auprès de la Chambre des représentants une Commission de la protection de la vie privée composée de … ».